IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	B.M. Jakobsson et al.
Case:	22-2
Serial No.:	09/538,663
Filing Date:	March 30, 2000
Group:	3691
Examiner:	Stefanos Karmis

Title: Methods of Protecting Against Spam Electronic Mail

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter referred to as "Appellants") hereby appeal the rejections of claims 1-6, 8-13 and 15-20 of the above referenced application.

Appellants note that the present appeal was initiated on September 16, 2005. Appellants would also like to point out that this is the fourth appeal brief filed in the present application. It is believed that the failure of the Examiner to permit the present application to proceed to the Board is resulting in an inefficient use of resources for Appellants and the U.S. Patent and Trademark Office, as well as an inordinate delay in prosecution.

The present application should be permitted to proceed to the Board for a decision on the merits.

The fee previously paid in conjunction with the Appeal Brief filed November 21, 2005 should be applied to the present Appeal Brief. Please charge the difference between the current fee and the amount previously paid to Ryan, Mason & Lewis, LLP Deposit Account No. 50-0762.

REAL PARTY IN INTEREST

The present application is assigned of record to Lucent Technologies Inc. On November 30, 2006, the assignee Lucent Technologies Inc. completed a merger with Alcatel S.A., with the resulting entity being named Alcatel-Lucent. Alcatel-Lucent is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

The present application was filed on March 30, 2000 with claims 1-20. A declaration under 37 C.F.R. §1.131, dated June 23, 2004, has established a priority date of April 2, 1999 for the claims.

Claims 7 and 14 have been canceled. Claims 1-6, 8-13 and 15-20 are pending in the present application. Claims 1 and 10 are the pending independent claims.

Claims 1, 10 and 17-20 stand rejected under 35 U.S.C. §102(e). Claims 2-6, 8-9, 11-13, 15 and 16 stand rejected under 35 U.S.C. §103(a).

Claims 1-6, 8-13 and 15-20 are appealed.

STATUS OF AMENDMENTS

An amendment was filed on September 20, 2007, solely to amend claims 18 and 20 in the manner suggested by the Examiner to overcome the objections raised in the Office Action dated July 6, 2007. This amendment was entered by the Examiner, as indicated on the Advisory Action dated November 14, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for preventing receipt by receivers of unwanted email sent by senders in a communication system. It is determined whether email to a receiver comprises valid message authentication code (MAC) information. Email directed to the receiver that does not comprise valid MAC information is filtered out at a gateway of the communication system. The receiver is provided with email directed to the receiver that comprises valid MAC information.

An illustrative embodiment of the recited method for preventing receipt by receivers of unwanted email sent by senders in a communication system (e.g., email system 10 in FIG. 1 that can be corrupted by spam email) is described in the specification at, for example, page 11, line 3, to page 14, line 12, with reference to FIG. 2. It is determined whether email to a receiver comprises valid MAC information (e.g., Specification, page 14, lines 1-7; Step 140 in FIG. 2; Specification, page 8, line 21, to page 9, line 5, "The validity of a MAC relies on knowing the secret key"). Email directed to the receiver that does not comprise valid MAC information is filtered out at a gateway of the communication system (e.g., Specification, page 14, lines 6-8; Step 160 in FIG. 2). The receiver is provided with email directed to the receiver that comprises valid MAC information (e.g., Specification, page 14, lines 6-8; Step 150 in FIG. 2).

Independent claim 10 is directed to a server for preventing receipt by receivers of unwanted email sent by senders in a communication system. A determining module determines whether email to a receiver comprises valid message authentication code (MAC) information. A filtering module filters out, at a gateway of the communication system, email directed to the receiver that does not comprise valid MAC information. A provisioning module provides the receiver with email directed to the receiver that comprises valid MAC information.

An illustrative embodiment of a server for preventing receipt by receivers of unwanted email sent by senders in a communication system (e.g., email system 10 in FIG. 1 that can be corrupted by spam email) is described in the specification at, for example, page 11, line 3, to page 14, line 12, with reference to FIG. 2. A determining module determines whether email to a receiver comprises valid MAC information (e.g., Specification, page 14, lines 1-7; Step 140 in FIG. 2; Specification, page 8, line 21, to page 9, line 5, "The validity of a MAC relies on knowing the secret key"). A filtering module filters out, at a gateway of the communication system, email directed to the receiver that does not comprise valid MAC information (e.g., Specification, page 14, lines 6-8; Step 160 in FIG. 2). A provisioning module provides the receiver with email directed to the receiver that comprises valid MAC information (e.g., Specification, page 14, lines 6-8; Step 150 in FIG. 2).

Techniques of preventing spam email in accordance with embodiments of the claimed invention provide efficient and computationally non-intensive authenticity verification of the email, thereby conserving the resources of the communication system. Additionally, embodiments of inventive techniques achieve message privacy using standard encryption methods and successfully manage data transmission problems associated with sending sensitive information by email. Such features, benefits and advantages have not heretofore been achieved in the art. See the specification at page 5, lines 16-22.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 1, 10 and 17-20 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,266,692 to Greenstein (hereinafter "Greenstein").

II. Claims 2, 3 and 11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Greenstein in view of Official Notice.

III. Claims 4-6, 8, 9, 12, 13, 15 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Greenstein in view of Official Notice, and further in view of U.S. Patent No. 6,546,416 to Kirsch (hereinafter "Kirsch").

ARGUMENT

Appellants incorporate by reference herein the disclosures of all previous responses filed in the present application, namely, responses dated June 24, 2004, January 26, 2005, August 17, 2005, November 21, 2005, May 15, 2006, September 29, 2006, and September 20, 2007. Sections I, II and III to follow will respectively address grounds I, II and III presented above.

I. Anticipation of claims 1, 10 and 17-20

A. Claims 1 and 10

Regarding the §102(e) rejection based on Greenstein, Appellants respectfully assert that Greenstein fails to teach or suggest all of the limitations in claims 1-6, 8-13 and 15-16 for at least the reasons presented in Appellants' previous responses as well as the reasons presented below.

It is well-established law that a claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Appellants respectfully assert that the rejection based on Greenstein does not meet this basic legal requirement.

In formulating the §102(e) rejection in the present Office Action at page 4, second paragraph, the Examiner argues that the passcode disclosed in Greenstein is analogous to the MAC recited in claim 1. Appellants respectfully disagree. The MAC recited in claim 1 is discussed and defined in the present specification at page 8, line 21, to page 9, line 5:

> [A] message authentication code (MAC) appended to the sender's M message will allow the message M to be received by receiver 40. This can be thought of as a secret password specific to the sender, receiver, and the sent email, and which only a sender who is registered can generate. More specifically, and as known in the art, a MAC is a keyed one-way function of an input wherein a secret key is known by both the generator and the verifier of the MAC. The validity of a MAC relies on knowing the secret key.

Thus, the MAC recited in claim 1 is a keyed one-way function of an input (e.g., the sent email) wherein a secret key is known by both the generator (e.g., the sender) and the verifier (e.g., the receiver). As such, the MAC of claim 1 is specific to a given message and is generated as an output of a function using a key specific to the sender and the receiver of that message. In contrast, Greenstein discloses the inclusion of a single passcode for all messages sent to a user by one or more senders, rather than the inclusion of a MAC, specific to a given message, generated using a key specific to the sender and the receiver of that message. See Greenstein at column 2, lines 24-35:

> The present invention enables the user, i.e., a would be recipient, to provide a "passcode" to all potential senders. The passcode may be a phrase which the user defines and sends to all welcome e-mail participants. The user would maintain a distribution list of valid senders to which the user can send an updated passcode easily. The passcode may either be an ASCII character stream, or a randomly generated binary "key." When sending an e-mail, a sender must specify the passcode which was provided by the recipient and which is inserted in a predefined field in a mail header. . . .

As discussed in the present specification at page 10, lines 9-13, the use of a MAC, as recited in claim 1, advantageously provides enhanced security:

> [T]he key is known only by the sender and intended receiver(s). An adversary will not be able to determine whether a given string is a valid MAC on a given message unless the adversary obtains access to the given key. This is true even after an arbitrary number of MACs for chosen messages other than m have been examined by the adversary.

Since Greenstein fails to teach the recited MAC information, Greenstein clearly fails to anticipate the limitations of claim 1 directed to the use of MAC information in the steps of determining, filtering, and providing emails to particular receivers. Thus, claim 1 is not anticipated by Greenstein and therefore recites patentable subject matter.

Claim 10 contains limitations similar to those recited in claim 1 and is thus patentable for at least the reasons identified above with reference to claim 1.

B. Claims 17 and 19

Dependent claims 17 and 19 are patentable at least by virtue of their dependency from independent claims 1 and 10. Moreover, these claims recite separately patentable subject matter. Specifically, dependent claims 17 and 19 recite limitations wherein a sender becomes a registered sender by satisfying a requirement. This limitation is described with regard to an illustrative embodiment in the present specification at, for example, page 5, lines 6-11:

> A sender becomes a registered sender by paying a price which will allow the sender to become a registered sender to the receiver. The price may be a monetary price, or some other computationally related price which is a function of the reservation of system resources. It may simply involve to register with some facility that monitors spamming and only certifies non-spammers, and refuses to renew certification of known offenders. Users registering may have to pay a deposit that is only returned if they are not found to abuse system resources.

In formulating the rejection of dependent claims 17 and 19 in the present Office Action at page 4, last paragraph, the Examiner relies primarily on Greenstein at column 2, lines 59-63:

> In addition, the present invention provides for the senders of the e-mail to request approval to send, e.g., request a valid passcode of the recipient, before sending the e-

> mail, thereby preventing senders from writing the e-mail first only to find that it is rejected.

The above portion of Greenstein fails to teach the limitation of claims 17 and 19 wherein a sender becomes a registered sender by <u>satisfying a requirement</u>; rather, it teaches away by disclosing that a sender merely needs to <u>request</u> approval to send.

<u>C. Claims 18 and 20</u>

Dependent claims 18 and 20 are patentable at least by virtue of their dependency from dependent claims 17 and 19, as well as from independent claims 1 and 10. Moreover, these claims recite separately patentable subject matter. Specifically, dependent claims 18 and 20 recite limitations directed to registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver.

In formulating the rejection of dependent claims 18 and 20 in the present Office Action at page 4, last paragraph, the Examiner relies primarily on Greenstein at column 2, lines 59-63:

> In addition, the present invention provides for the senders of the e-mail to request approval to send, e.g., request a valid passcode of the recipient, before sending the e-mail, thereby preventing senders from writing the e-mail first only to find that it is rejected.

Appellants respectfully submit that the above-quoted portion of Greenstein not only fails to teach registering the particular sender <u>when the particular sender is determined not to be a registered sender of email to the particular receiver</u>, but in fact teaches away by disclosing an alternative technique wherein senders request approval to send <u>before</u> sending e-mail.

Greenstein further teaches away by disclosing an alternative technique wherein, if a sender does not have a passcode, the user is prompted to authorize a single e-mail, rather than providing a passcode to the sender. See Greenstein at, for example, column 1, lines 50-53 ("The email without valid passcodes may either be deleted or stored temporarily. In the latter case, an approval request to the recipient will be initiated to verify the rejection of the email."), and at column 3, lines 52-61:

> At step 114, if a sender did not specify a passcode when sending to the user who requires such passcode, the server stores the e-mail in a temporary storage, i.e., a holding tank, at step 116. At step 118, the server transmits an authorization request to the user via the mail client, to either accept or reject the e-mail. If the user approves the e-mail at step 120, the e-mail is placed in the mail database at step 110, making it available to the mail client to retrieve at step 112. On the other hand, if the user rejects the e-mail at step 122, the e-mail is deleted at step 126.

II. Obviousness of claims 2, 3 and 11

A. Claim 2

Dependent claim 2 is patentable at least by virtue of its dependency from independent claim 1. The patentability of claim 1 has been described above. However, dependent claim 2 also recites patentable subject matter in its own right.

In formulating the present rejection of claim 2 on page 5, last paragraph, of the Office Action, the Examiner concedes that "Greenstein fails to teach registering a sender by establishing a cookie which indicates to the particular receiver whether the particular sender has satisfied the requirement to allow the particular sender to become a registered sender. Official Notice is taken that cookies are old and well known in the computer arts."

The Examiner relies on Official Notice without any evidentiary support for any use of a cookie, much less the use of a cookie in the manner claimed, as the primary grounds to reject claim 2. MPEP 2144.03 states that "[i]t is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based." Appellants respectfully submit that the application of official notice to reject claims 2, in the absence of any evidentiary showing, fails to comply with this instruction. Moreover, the Examiner has failed to provide either documentary evidence or an affidavit or declaration setting forth specific factual statements and explanation to support the invocation of official notice, as required by 37 C.F.R. §1.04(d)(2) in order for such a rejection to be maintained.

Moreover, Appellants assert that even if one accepts the Examiner's assertion that the general concept of cookies is well known in the art, the specific limitations of claim 2 are not obvious in light of Greenstein and this general concept of cookies. For example, page 12, lines 8-9, defines the term "cookie," as recited in claim 2, as "a message that provides evidence that an initiator of the cookie paid the required setup cost or that it will be possible to force sender S to pay the setup cost."

Nowhere does Greenstein teach establishing a cookie, or an equivalent, that indicates to the particular receiver whether the particular sender has satisfied a requirement to allow the particular sender to become a registered sender to the particular receiver. Therefore, Appellants respectfully submit that Official Notice of a general concept of a cookie fails to remedy the fundamental deficiency of Greenstein to reach the limitations of claim 2.

Moreover, the Examiner further argues that Greenstein teaches establishing an address related to an address associated with the particular receiver which will inform the particular sender that the particular receiver desires that the particular sender be able to send email to the particular receiver. This limitation is described in the specification with regard to an illustrative embodiment at, for example, page 14, lines 1-7:

> At step 140 it is determined whether the email m is valid according to a processed MAC. It is preferable to determine an extension e of receiver R's email address such that when this extension appears in the email, receiver R will accept the mail. Letting μ = hash(m), e is defined as MAC $K_{RS}(\mu)$. Receiver R then computes KRS for the alleged senders of the email and calculates e. The email is accepted at step 150 if and only if the same extension of receiver R's address is the same as the result calculated for e.

In formulating the rejection of claim 2 in the present Office Action, the Examiner argues that this limitation of establishing an address related to an address associated with the particular receiver is met by FIG. 3 of Greenstein, which the Examiner alleges shows "that the passcode is part of the address for sending the email." Appellants respectfully disagree with the Examiner's characterization of FIG. 3 of Greenstein. Rather, FIG. 3 of Greenstein clearly shows that the passcode is included as a header field distinct from the address associated with the particular receiver. See Greenstein at column 4, lines 22-31:

> [T]he incoming e-mail header needs to include a header field reserved for the passcode. The e-mail server compares this header field with the passcode profile 404 for the user when validating the passcode.
>
> The e-mail client 420 is configured to support an additional passcode field. This field is similar to, e.g., TO, FROM, CC, SUBJECT fields. An example of a sample e-mail page 302 including the passcode field 304 is shown in FIG. 3.

Moreover, the present specification explicitly distinguishes the technique recited in claim 2 from that disclosed in Greenstein. See, e.g., the present specification at page 14, lines 11-12 ("Alternatively at step 140, instead of using an address extension, the MAC can be communicated in an available header of the email."). Once again, the Examiner's Official Notice of a cookie does not remedy the deficient teaching of Greenstein; therefore, Appellants believe that the cited references do not render claim 2 obvious.

Moreover, in formulating the rejection of claim 2, the Examiner asserts that "it would have been obvious to one of ordinary skill in the art at the time of the Appellant's invention to modify the teachings of Greenstein to include cookies because it allows for faster authentication of emails when communicating between computers." Appellants respectfully submit that the proffered statement fails to provide sufficient objective motivation for the proposed modification of Greenstein and, rather, is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. KSR v. Teleflex, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007), quoting In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

More specifically, the statement above is using the benefit obtained from a modification as a motivation for that combination and thus constitutes impermissible hindsight. See, e.g., KSR v. Teleflex, 127 S.Ct. at 1742 ("A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."); Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 36 (1966) (cautioning factfinders "to resist the temptation to read into the prior art the teachings of the invention in issue").

In order to avoid the improper use of a hindsight-based obviousness analysis, particular findings must be made as to why one skilled in the relevant art, having no knowledge of the claimed invention, would have modified the teachings of Greenstein in the manner claimed . See, e.g., In re Kotzab, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000). The Examiner's conclusory statements do not adequately address the issue of motivation to combine references. "It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" In re Sang-Su Lee, 277 F.3d 1338, 1344 (Fed. Cir. 2002) (quoting W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983)).

For at least these reasons, Appellants assert that a *prima facie* case of obviousness has not been established. Therefore, Appellants respectfully request that the §103(a) rejection of claim 2 be withdrawn.

B. Claims 3 and 11

Dependent claims 3 and 11 are patentable at least by virtue of their dependency from independent claims 1 and 10. The patentability of claims 1 and 10 have been described above. Further, dependent claim 3 is patentable at least by virtue of its dependency from dependent claim 2. The patentability of claim 2 has been described above. In addition, dependent claims 3 and 11 also recite patentable subject matter in their own right.

Dependent claims 3 and 11 recite limitations directed toward establishing an address by generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender and the particular receiver. An illustrative embodiment of the claimed arrangement utilizes a stream cipher generated random sequence, which is generated using a pseudorandom function that uses a keyed hash function. See the specification at page 12, lines 1-19.

In contrast to the Examiner's argument, Greenstein does not teach generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the sender and receiver. Rather, Greenstein merely discloses that a passcode may be, for example, "a randomly generated binary 'key'." See Greenstein at column 2, lines 30-32. This basic description does not teach or suggest a pseudorandom function with a keyed hash function. Furthermore, the Examiner's invocation of Official Notice of a cookie does not remedy the deficient teaching of Greenstein with regard to a pseudorandom function with a keyed hash function; therefore, Appellants believe that the cited references do not render claims 3 and 11 obvious.

III. Obviousness of claims 4-6, 8, 9, 12, 13, 15 and 16

A. Claims 4, 8, 9, 15 and 16

Dependent claims 4, 8, 9, 15 and 16 are patentable at least by virtue of their dependency from independent claim 10 and dependent claim 2. The patentability of claims 2 and 10 have been described above. Moreover, claims 4, 8, 9, 15 and 16 recite separately patentable subject matter.

In formulating the rejections of these claims in the present Office Action at page 6, last paragraph, the Examiner asserts that "[i]t would have been obvious to one of ordinary skill in the art to modify the teachings of Greenstein in view of Official Notice with the public key encryption teachings of Kirsch because it allows for authenticating emails effectively when filtering emails with the motivation of removing unwanted emails."

Appellants respectfully submit that the proffered statement fails to provide sufficient objective motivation for the proposed combination. Appellants respectfully note that none of claims 8, 9, 13, 15 and 16 mention any use of public key encryption. As such, it is at best unclear as to why would be motivated to modify reference teachings with public key encryption teachings so as to reach a technique which does not involve public key encryption.

Moreover, the above-quoted statement is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. KSR v. Teleflex, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007), quoting In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

More specifically, the statement above is using the benefit obtained from a combination as a motivation for that combination and thus constitutes impermissible hindsight. See, e.g., KSR v. Teleflex, 127 S.Ct. at 1742 ("A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."); Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 36 (1966) (cautioning factfinders "to resist the temptation to read into the prior art the teachings of the invention in issue").

In order to avoid the improper use of a hindsight-based obviousness analysis, particular findings must be made as to why one skilled in the relevant art, having no knowledge of the claimed invention, would have combined the teachings of the references in the manner claimed. See, e.g., In re Kotzab, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000). The Examiner's conclusory statements do not adequately address the issue of motivation to combine references. "It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" In re Sang-Su Lee, 277 F.3d 1338, 1344 (Fed. Cir. 2002) (quoting W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983)).

For at least these reasons, Appellants assert that a *prima facie* case of obviousness has not been established. Therefore, Appellants respectfully request that the §103(a) rejection of claims 4, 8, 9, 15 and 16 be withdrawn.

B. Claims 5, 6 and 13

Dependent claims 5, 6 and 13 are patentable at least by virtue of their dependency from independent claim 10 and dependent claim 2. The patentability of claims 2 and 10 have been described above. Moreover, claims 5, 6 and 13 define separately patentable subject matter.

Claims 5 and 13 recite limitations wherein registration of a sender comprises sending to a particular user by a particular receiver an encrypted key, wherein the encrypted key is a member of a set of encrypted keys.

In the present Office Action at page 6, last paragraph, the Examiner concedes that Greenstein fails to teach the use of encryption. The Examiner suggests that this deficiency may be remedied by Kirsch at column 6, line 51, to column 7, line 12, which the Examiner characterizes as teaching "a method and system for selectively blocking delivery of bulk electronic mail utilizing public key encryption as well as other encoding and encrypting algorithms."

Appellants respectfully submit that the relied-upon portion of Kirsch is directed toward a technique wherein a digital signature provided in a challenge message may be formed utilizing any conventional encoding or encrypting technology, including public key encryption. See Kirsch at column 6, lines 51-58. Appellants respectfully submit that the digital signature disclosed by Kirsch is not itself a key, much less a member of a set of keys, but rather itself comprises encrypted data. See, e.g., Kirsch at column 10, lines 25-41:

> [E]-mail messages not yet accepted or rejected, are then evaluated 77 to determine whether the message contains a signature recognizable by the system 60. The signature, where found, is decoded or decrypted 80 depending on the nature of the signature identified. In accordance with alternate preferred embodiments of the present invention, the identification of the signature may depend entirely on an algorithmic evaluation of the signature block itself or upon data included in the challenge list 28'. In the latter circumstance, the challenge list 28', may be used to record information identifying different possible types of signatures and, thereby, the corresponding decoding and decrypting algorithms, the scope of pre-existing content utilized in the generation of the signature, and other information usable in identifying whether the particular received e-mail message and its signature were originated by the system 60.

As such, the combination of Greenstein and Kirsch, as well as the aforementioned Official Notice of cookies, fails to reach the limitations of claims 5 and 13 wherein registration of a sender comprises sending to a particular user by a particular receiver an encrypted key, wherein the encrypted key is a member of a set of encrypted keys.

Moreover, as noted above with reference to dependent claims 4, 8, 9, 15 and 16, the Examiner has failed to provide sufficient objective motivation for the proposed combination and instead attempted to premise the rejections on a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. KSR v. Teleflex, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007), quoting In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

For at least these reasons, Appellants assert that a *prima facie* case of obviousness has not been established with regard to claims 5 and 13. Moreoever, claim 6 is believed patentable at least by virtue of its dependency from claim 5. Therefore, Appellants respectfully request that the §103(a) rejection of claims 5, 6 and 13 be withdrawn.

B. Claim 12

Dependent claim 12 is patentable at least by virtue of its dependency from independent claim 10, the patentability of which has been described above. Moreover, claim 12 recites separately patentable subject matter. Specifically, claim 12 recites a limitation wherein a registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption.

As discussed above with reference to claim 2, the Examiner contends that FIG. 3 of Greenstein teaches "that the passcode is part of the address for sending the email." However, in the present Office Action at page 6, last paragraph, the Examiner concedes that Greenstein fails to teach the use of encryption. The Examiner suggests that this deficiency may be remedied by Kirsch at column 6, line 51, to column 7, line 12, which the Examiner characterizes as teaching "a method and system for selectively blocking delivery of bulk electronic mail utilizing public key encryption as well as other encoding and encrypting algorithms."

Appellants respectfully submit that the combination of the alleged teaching of Greenstein "that the passcode is part of the address for sending the email" and the alleged teachings of Kirsch directed toward "selectively blocking delivery of bulk electronic mail utilizing public key encryption" fail to reach the limitations of claim 12 wherein a registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption. The Official Notice taken by the Examiner regarding the use of a cookie fail to remedy this deficiency.

Moreover, as noted above with reference to claim 2, Greenstein in fact teaches a technique wherein a passcode is included as a header field distinct from the address associated with the particular receiver. Likewise, the relied-upon portion of Kirsch is in fact directed toward a technique wherein a digital signature provided in a challenge message may be formed utilizing any conventional encoding or encrypting technology, including Public Key Encryption. See Kirsch at column 6, lines 51-58. This only further underscores the fact that Greenstein and Kirsch cannot be combined with Official Notice regarding the use of a cookie in the manner suggested by the Examiner so as to reach the limitations of claim 12.

Moreover, as noted above with reference to dependent claims 4, 8, 9, 15 and 16, the Examiner has failed to provide sufficient objective motivation for the proposed combination and instead attempted to premise the rejections on a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. KSR v. Teleflex, 127 S.Ct. 1727, 1741, 82 USPQ2d

1385, 1396 (2007), quoting In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

For at least these reasons, Appellants assert that a *prima facie* case of obviousness has not been established. Therefore, Appellants respectfully request that the §103(a) rejection of claim 12 be withdrawn.

For the reasons stated above, Appellants respectfully request withdrawal of the §102(e) rejections of claims 1, 10, and 17-20, and the §103(a) rejections of claims 2-6, 8-9, 11-13, and 15-16. The present application is believed to be in condition for allowance, and such favorable action is respectfully solicited.

Respectfully submitted,

Date: November 16, 2007

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising the steps of:

determining whether email to a particular receiver comprises valid message authentication code (MAC) information;

filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information; and

providing the particular receiver with email directed to the particular receiver that comprises valid MAC information.

2. The method of claim 18, wherein the step of registering the particular sender comprises the steps of:

establishing by the particular sender a cookie which indicates to the particular receiver whether the particular sender has satisfied the requirement to allow the particular sender to become a registered sender to the particular receiver;

establishing an address related to an address associated with the particular receiver which will inform the particular sender that the particular receiver desires that the particular sender be able to send email to the particular receiver; and

establishing by the particular receiver a key which is forwarded to the particular sender by the particular receiver to inform the particular sender that the particular sender is authorized to send email to the particular receiver and is now a registered sender and for use by the particular sender whenever the particular sender wishes to send email to the particular receiver.

3. The method recited in claim 2, wherein said step of establishing the address comprises generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

4. The method recited in claim 2, wherein said step of establishing an address comprises sending email from the particular receiver to the particular sender using public key encryption.

5. The method recited in claim 2, wherein said registering step further comprises sending to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

6. The method recited in claim 5, further comprising the step of storing the encrypted key by the particular sender in a table of encrypted keys for use by the particular sender whenever the particular sender desires to send email to the particular receiver.

8. The method of claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC against a value determined by the particular receiver.

9. The method recited in claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

10. A server for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising:

a determining module for determining whether email to a particular receiver comprises valid message authentication code (MAC) information;

a filtering module for filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information; and

a provisioning module for providing the particular receiver with email directed to the particular receiver that comprises valid MAC information.

11. The server recited in claim 20, wherein said registering module further comprises a generator for generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

12. The server recited in claim 11, wherein said registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption.

13. The server recited in claim 11, wherein said registering module sends to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

15. The server of claim 10, wherein said filtering module compares the MAC against a value.

16. The server recited in claim 15, wherein the filtering module compares the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

17. The method of claim 1, further comprising the step of determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement.

18. The method of claim 17, further comprising the step of registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver.

19. The server of claim 10, further comprising a registering module for determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement.

20. The server of claim 19, wherein the registering module is also for registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver.

EVIDENCE APPENDIX

Attached hereto is a Declaration Under 37 C.F.R. §1.131 and accompanying Exhibits A-J, originally submitted on June 24, 2004.

Attorney Docket # 4167-242

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Jakobsson, et al.
Serial No.: 09/538,663
Filed: March 30, 2000
For: Methods of Protecting Against Spam Electronic Mail

DECLARATION UNDER37 C.F.R. §1.131

I, Bjorn Marcus Jakobsson, declare as follows:

1. This declaration is submitted in support of U.S. Patent Application Serial Number 09/538,663 and, specifically to establish conception of the invention in the United States prior to the March 10, 2000 filing date of U.S. Patent No. 6,691,156 ("Drummond"), the reference cited by the Examiner in rejecting the claims under 35 U.S.C. §102(e), and to establish reasonable diligence in the period between the conception and filing of the subject patent application.

2. The subject patent application was filed on March 30, 2000, which is the constructive reduction to practice date of the subject invention.

3. From the period prior to March 10, 2000 until the application was filed, applicants were, in conjunction with their attorneys, diligently preparing the subject application for filing in the United States Patent and Trademark Office.

4. The invention which is the subject of this patent application was conceived by me prior to April 2, 1999. On or before April 2, 1999, a full description of the invention in the form of a manuscript was submitted to my department supervisor, A. Silberschatz, at Lucent Technologies for consideration as the subject of possible patent protection. I created the manuscript in preparation for a proposed talk to be held on September 20, 1999 at Communications and Multimedia Security in Leuven, Belgium. A copy of the manuscript is attached hereto as Exhibit A.

5. On April 2, 1999, A. Silberschatz summarized my disclosure in a letter to Jeffrey Weinick of the Lucent Technologies patent review department. A copy of A. Silberschatz' letter to Jeffrey Weinick, bearing the date of April 2, 1999, is attached hereto as Exhibit B.

6. Copies of A. Silberschatz' April 2, 1999 letter were also provided to me and, upon their receipt, I forwarded the above-referenced manuscript to Jeffrey Weinick for his review, together with a "Request for Approval of Manuscript" dated April 7, 1999. A copy of the "Request for Approval of Manuscript" is attached hereto as Exhibit C.

7. The manuscript of Exhibit A discloses all of the essential subject matter of the present application upon which the claims of the application are based.

8. In the Spring of 1999, the invention was in thc patent review process within Lucent, which typically receives from its employees approximately 60 to 70 submissions of inventions per month. The subject invention was assigned a submission number and handled in turn.

9. In May of 1999, Lucent's file relating to my invention and containing the disclosure of Exhibit A was submitted to Eli Weiss, Corporate Counsel for the Intellectual Property Law Department of Lucent Technologies, who sent the file (now assigned Lucent Technologies IDS ("invention disclosure submission") number 118626 to Lucent Technologies outside patent counsel, the firm of Cohen, Pontani, Lieberman and Pavane, for preparation and filing of the subject application. A copy of the transmittal letter forwarding the disclosure to Cohen, Pontani, Lieberman and Pavane is attached hereto as Exhibit D.

10. Shortly after the disclosure file was sent to Cohen, Pontani, Lieberman and Pavane for preparation of a patent application on my invention, we were contacted by Jeffrey Navon, an attorney at Cohen, Pontani, Lieberman and Pavane, to discuss the invention so that a patent application could be prepared. Mr. Navon provided me with a draft patent application on October 15, 1999, and rcquested that I review it and provide him with comments. A copy of Mr. Navon's facsimile transmission sheet requesting my review of the draft application is attached hereto as Exhibit E.

11. I reviewed the first draft of the patent application and provided Mr. Navon with our comments during the first week of December 1999. In an email dated December 7, 1999, Mr. Navon indicated that he received my comments and would send me a revised draft later in the week. A copy of Mr. Navon's email of December 7, 1999 is attached hereto as Exhibit F.

12. In a letter dated February 9, 2000, Mr. Weinick established a new, non-extendible filing date of March 30, 2000 for my patent application. Mr. Weinick's letter was addressed to Lance Lieberman, a partner at Cohen Pontani, Lieberman and Pavane who is responsible for managing Lucent cases. A copy of Mr. Weinick's letter is attached hereto as Exhibit G.

13. On March 10, 2000, I completed my review of the revised patent application draft and emailed my comments to Mr. Navon. A copy of our email of March 10, 2000 is attached hereto as Exhibit H.

14. On March 22, 2000, I completed my review of a further revised patent application draft and emailed my comments to Mr. Navon. A copy of my email of March 22, 2000 is attached hereto as Exhibit I.

15. Mr. Navon incorporated my comments into a finalized draft which was filed with the United States Patent and Trademark Office on March 30, 2000. In a letter dated April 3, 2000, Mr. Lieberman indicated that the application was filed in unexecuted condition, and forwarded

a Declaration and Assignment to me for signature. A copy of Mr. Lieberman's letter of April 3, 2000 is attached hereto as Exhibit J.

16. As is clear from the foregoing, applicants and those involved in preparing and filing the subject application on applicants' behalf, have exercised reasonable diligence from prior to the March 10, 2000 filing date of the cited Drummond patent (i.e., from April 2, 1999) up to the filing date of this application. Accordingly, the Examiner's rejection under 35 USC 102(e) should be withdrawn.

17. I declare that all statements made herein of my own knowledge are true; that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this patent application and any patent resulting therefrom.

Date: Jun 23 '04

By: ______________________
Bjorn Marcus Jakobsson

EXHIBIT A

How to Protect Against a Militant Spammer

Markus Jakobsson[*] Joy Müller[†]

Abstract

We consider how to avoid unsolicited email – so called *spam* – in a stronger adversarial model than what has previously been considered. Our primary concern is the proposal of an architecture and of protocols preventing against successful spamming attacks launched by a strong attacker. This attacker is assumed to control the communication media and to be capable of corrupting large numbers of protocol participants. Secondly, we show how services such as message integrity and message privacy can be obtained virtually for free by using the structures put in place for spam protection. A final issue we are concerned with is how to produce protocols that have the property that the bulk of the computational requirements and storage requirements are shifted towards one of the participants, in order to reflect the desired power balance and to avoid denial-of-service attacks. This results in a simple and efficient solution that is largely backwards-compatible, and which addresses many of the concerns surrounding email communication.

Keywords: authentication, light-weight, spam, strong adversary

1 Introduction

To many people, email is becoming a crucial tool of daily life, much like the car became an integral part of life for many families some decades ago. Email, in fact, to some extent is a substitute for the car, in terms of allowing telecommuting and quick delivery of information. For both of these vehicles of the twentieth century, there is a need for traffic rules and enforcement of the same. Clearly, we would not tolerate a truck parked in the middle of an intersection, the driver handing out flyers. By the same token, there is no reason why the same behavior in the digital domain should be accepted. Until quite recently, though, there has been no suggestion of how to enforce good behavior on the digital roads.

[*] Information Sciences Research Center, Bell Laboratories, Murray Hill, NJ 07974, markusj@research.bell-labs.com

[†] Johannes Gutenberg Universität Mainz, Fachbereich Mathematik, 55128 Mainz, joy@dialup.nacamar.de

A recent upswing in the amount of *spam*, i.e., email broadcast advertisements, has caused both considerable congestion and concern, particularly in light of how inexpensive and efficient the spamming methods are, and the ease with which spammers have been able to avoid having their outgoing traffic filtered out, by moving from domain to domain and by disguising themselves. In [10], Gabber et al suggested a method for categorizing email, allowing unrequested email to be automatically erased without consuming any system resources or user time. However, their model assumes a rather "nice" adversary: The spammer in their model is only assumed to use today's methods of acquiring email addresses, namely to either buy lists of valid email addresses or collect these from newsgroups, etc. Given that their solution – if employed – makes the efforts of such a spammer completely meaningless, it is likely that the warfare is stepped up, and a new breed of more militant spammers becomes common.

It is the aim of this work to defend against this more aggressive type of behavior just as the spammer with today's methods was defended against in [10]. We propose a new, stronger adversarial model, and propose an efficient solution that meets the adversarial model and that makes the efforts of the militant spammer almost pointless. Here, the word "almost" is important: it is necessary to allow for normal email traffic, and allow two entities that have not previously established a communication link to communicate with each other (or the strength of email will be severely reduced), so it will still be possible for a spammer to send advertisements in a very well targeted manner. We mean that this is not unreasonable, though, since it shifts the effects of the spammer from an instigator of traffic jams to an advertiser that only sends very well directed advertisements in significantly lower quantities.

Before we discuss the new adversarial model, let us linger briefly on the model and solution of [10]. There, a spammer is assumed to obtain email addresses only by compromising servers holding valid addresses (this models both getting email addresses from newsgroups, and buying them from companies compiling email address lists, and similar approaches.) The solution suggested is to use *extended addresses*, which consists of the "normal" addresses (the so called *core* address) and an extension. The extension is a sequence of characters acting like a password for the email to be accepted, where the extension used by one pair or participants cannot be guessed from a set of other extensions. An extension may only be obtained by sending a request (of a special format that cannot be used for spam) to the desired receiver of an email message; the request may contain a proof of having performed a certain computational task, particular to the pair of sender and receiver (thus implementing a cost for each connection to be set up). Similarly, it may contain a proof of a monetary expense, such as an attached digital coin whose validity can easily be verified and which may be cashed as a "punishment" for spamming.

Consider now an attacker that is allowed to eavesdrop on communication lines, and who may collect valid extensions when he sees them, either in a response to a request for an extension, or more straightforwardly, from the address fields of valid messages passing from the senders to the receivers. He may then use these extensions, possibly masquerading as the sender he "stole" the extension from. Even though it clearly makes the compilation of address lists more elaborate, the attack is far from difficult to perform; in fact, the only reason why this approach is not used today already is probably that it is slightly simpler to collect addresses from newsgroups, etc.

An even more aggressive attacker is allowed the following, ultimate, attack as well: he may, apart from eavesdropping on the communication lines, also perform substitution attacks, viz. substitute a legal email with his advertisement (wherein he may keep parts of the old message, such as the sender and receiver information, and the extension employed therein.) In other words, this militant breed of spammer may monitor network traffic, and adaptively insert and substitute messages, hoping to succeed in making a receiver accept a message that was not sent from a party from whom the receiver desires email.

We suggest an efficient and structurally very simple solution that protects against an adversary of the above type. It relies only on very conventional and well analysed cryptographic functions. Our solution is efficient in terms of storage, communication, and computation. Moreover, and also importantly, the solution is largely backwards-compatible with existing methods, and allows for a gradual implementation (in the sense that some entities may choose to employ the scheme, while others do not.)

Note that we consciously shift the computational and storage requirements towards the senders of the emails, in order to make the load of the receivers lighter. This serves a dual purpose: First, to discourage spam, and second, to limit the risk of a denial-of-service attack (see e.g., [14] for related issues and methods).

Organization: We present our goals in section 2, and review related work in section 3. After specifying the model and requirements in section 4, we list what building blocks will be used in section 5, and finally we present our solution in section 6. In the Appendix, we prove our solution to satisfy our requirements based on the assumptions.

2 Goals

We will now informally describe the desired requirements we want our solution to satisfy, given the adversarial model to be considered:

Only messages originating from *registered* senders will be delivered; all other messages will be weeded out at the gateway of the receiver. A party becomes registered by paying an agreed-upon price, which may be either a computational or monetary cost. It must not be possible to substantially reduce the price per working connection. (This allows us to establish lower bounds on the costs of spamming.) Furthermore, a message recipient can retract the registration of

invention

any sender at any time, thereby forcing spammers to pay the price of becoming registered for each email message to be sent. The receiver may also implement a categorization of senders, allowing sorting of messages according to meaning, context and priority.

Note that our suggested solution will, as a side-effect, allow us to provide authenticity verification of the messages virtually for free. This means that the receiver will be able to determine whether the received message was indeed sent from the claimed sender. The authentication can be either relative to a pseudonym (for which the identity of the owner is not known), or relative to a certified identity. The former is trivially obtained using our proposed solution, and the latter can easily be obtained if the sender has a public key registered, allowing her to prove knowledge of the corresponding secret key during the setup phase (which only occurs once for each pair of participants.) Note also that the authentication feature does not allow the receiver to convince a third party of the authenticity of a given message (without the implicit cooperation of the sender), i.e., we obtain *private authentication*[1] of messages. (If this property is not desired, then standard digital signature methods can be applied on a per-message basis.) Whereas neither authentication nor private authentication are primary goals of our investigation, they constitute an additional bonus of employing our method. Finally, it is easy to obtain message privacy (using standard encryption methods) by employing the structures already used for the spamming protection. Therefore, our solution, while not cryptographically advanced, successfully manages to solve an array of related and functionally interdependent real-world problems, whose exact relations have not previously been clarified. The contribution of our work should be seen in terms of the practical issues it addresses, and in the clean and simple solution it provides.

3 Related Work

The conceptually perhaps simplest and least intrusive approach to spamming prevention, and the absolutely most commonly used method, is filtering according to senders' addresses and according to message and subject keywords. However, it is not very efficient, as it is easily foiled by adversaries avoiding particular keywords known to be black-listed, and avoiding to use (or camouflaging the use of) certain black-listed sender addresses or domains.

A solution that better prevents against spam is to use electronic mail channel identifiers [11]: A receiver assigns a different channel to each sender by giving each of them a unique email address at which to contact him. Incoming mail gets sorted or rejected according to the address sent to and the sender they originate from. Mails originating from unknown senders may be put in a "public" channel. (These public channels are therefore not spam-free.)

[1] See, e.g., [13] for a description and solution of a similar concept relating to signatures.

A related approach is to use secret extensions of email addresses (which in principle are sender-recipient unique passwords appended to the recipient user name) instead of different channels. This is done in the scheme by Gabber et al [10]. There, spamming-prevention is done by filtering the incoming mails according to the extension, discarding emails without a valid extension. The weaknesses of both [10] and [11] stem from the fact that the "passwords" are communicated in the clear, allowing an eavesdropping adversary to circumvent the security measures. A difference between [10] and [11] is that Gabber et al employ computational puzzles to inflict a computational cost on anybody who wants to be given a valid extension.

The idea to require computational payments was first proposed by Dwork and Naor [6]. This was also the first paper to consider how to prevent against spam using cryptographic methods. In [6], an email has to be accompanied by a correctly evaluated *medium-hard function* (later also called a *puzzle*) in order to be accepted. In contrast, the solution by [10] only requires this setup to be performed once for each pair of communicating participants, which allows the computational cost to be raised without causing communication havoc. (This is an advantage, as by requiring higher computational costs, spamming is further discouraged.)

After the introduction of puzzles in [6], different solutions have been studied by Franklin and Malkhi [9], Gabber et al [10], and Juels [14], each paper proposing variants with different properties. These papers also use the resulting functions in different contexts, ranging from advertising to prevention of denial-of-service attacks.

The spam problem was also given attention by Cranor and LaMacchia [5], who reviewed the previously mentioned solutions and presented an outline of some regulatory solutions from the legislative realm.

All of the above solutions allow an adversary to steal information from messages that allows him later to spam, or to replace portions of messages so that they *become* spam. We consider a stronger model than what previous work does, to avoid these problems.

A central building block in our scheme is the message authentication code (MAC for short). A MAC is a keyed one-way function of the input, where the secret key is known by both the generator and the verifier of the MAC, and the validity of the MAC (corresponding to the authenticity of its input) relies on knowing the secret key. We refer to [22] for a review of MACs. An early description of a MAC construction based on a hash function was made by Tsudik in [23]. Preneel and van Oorschot [19] pointed out some problems of this construction, which was later studied and strengthened by Bellare, Canetti and Krawczyk [2]. In the latter paper, a hash-function based MAC design is proposed and proven to be secure based on general cryptographic assumptions.

Another building block in our scheme is the one-time pad. We use this for a realization of encrypted return-channels that allows the computational burden to be shifted from the recipient of a message to the originator, and allows the recipient to return encrypted messages with a minimum of effort. Note, however, that the one-time pads are generated as the outputs of a pseudo-random function and communicated encrypted using standard public key methods. (Thus, the one-time pad is only as secure as its building blocks, and is not information-theoretically secure as one-time pads are when truly random and communicated out-of-band.)

4 Model and Requirements

In our model, participants are modelled as senders and receivers, where each participant may alternatingly play both of these roles. We denote the sender Sally with S, and her intended receiver Ray with R. In our model, a participant is therefore a computational device, and this can be modelled by a polynomial-time Turing Machine. A *user* is the human or program with access to the machine that corresponds to a participant. For a user to be presented with an email M along with a label describing its sender S, M must first be *accepted* by the receiver R corresponding to this user. In turn, for a receiver R to accept an email M from a sender S, an entry describing the latter needs to be in a list of wanted senders with R. Descriptions of participants get added to this list by paying a setup cost C, but may be removed from the list by R if R (or its corresponding user) so decides. When this occurs, no more messages from S will be accepted by R, and no more messages from S will be displayed to the user (including those already accepted but not already displayed.)

Adversary. An adversary is a party who may corrupt any number of participants. When a participant is corrupted, the entire memory contents and computational resources are made available to the adversary, who also controls what messages are sent by the corrupted party. It is assumed that the adversary can not influence the actions of a participant who is not corrupted. Additionally, the adversary controls the communication channel, and may remove and inject messages at will. He can read all communication between non-corrupted participants. We model the latter by the (stronger) adversarial model in which the adversary may chose a polynomial number of messages and have the MACs of these computed by an oracle before he attempts to perform an attack. (Note, however, that the adversary may not include one of the MACs obtained from the oracle in any of the messages he causes to be sent.) The adversary has the following goals:

Spamming attack: One goal of the adversary is to make some k non-corrupted participants $\mathrm{R}_1 \ldots \mathrm{R}_k$ accept each one message $M_1 \ldots M_k$, where these messages are chosen by the adversary, without the adversary having to pay a total cost close to or exceeding $(k - k')C$, where k' is the number of the above messages that are labelled as being sent by a participant who is corrupted.

Authentication attack: A second goal of the adversary is to make a receiver R accept an email M and present this to the user as originating from a non-corrupted participant S, when in fact the message did not originate from S.

Sender privacy attack: A third goal of the adversary is to convince a non-corrupted participant that a message M was sent by a non-corrupted sender S to some (potentially corrupted) receiver R.

Message privacy attack: The fourth and final goal of the attacker is to determine whether a first message M_1 or a second message M_2 was sent between two non-corrupted participants. More formally, this corresponds to a successful chosen ciphertext attack (see, e.g., [3] for a detailed treatment.)

We require that an adversary cannot succeed with the above attacks with more than a negligible probability. More specifically, except with a negligible probability, an adversary cannot (1) succeed with a *spamming attack*; (2) succeed with an *authentication attack*; (3) succeed with a *sender privacy attack*; or (4) succeed with a *message privacy attack*.

5 Building Blocks and Assumptions

Authentication: As an authentication mechanism we use so-called message authentication codes, which we use both to *validate* and *authenticate* the transmitted messages. The MAC can be based on a keyed cryptographic hash function h, where the key is known (only) by the sender and the intended receiver(s). We require that it must be a hard problem to determine whether a given string is a valid MAC on a given message m, unless the verifier has access to the secret key. This must hold even after a polynomial number of MACs for chosen messages (other than m) have been seen. The security of the authentication mechanism relies on the assumptions on the underlying hash function. It has been shown that for this to hold, it is sufficient and necessary that it is hard to compute the output of the hash function without knowledge of the secret key, and that the hash function must be (weakly) resistant to collision finding. (We refer to [1, 2] for a thorough treatment.)

In addition to these basic properties, we assume that the hash function h can be modelled by a random oracle [4], in order to use it for key generation purposes. (This assumption may be replaced by another if we use another method for key generation.)

In practice, it is believed that MD5 [20] and SHA-1 [17] have the desired properties required for the hash function.

One-Time Pad: P denotes a one-time pad, which is generated by a pseudo-random function generator, e.g., using a keyed hash function h on an input which is a unique serial number.

Symmetric Encryption: To achieve privacy we use a symmetric encryption, such as the DES [15] or the proposed AES. We assume the symmetric encryption to be secure against chosen cipher text attacks.

Public-Key Encryption: For the protocol we use a public-key encryption scheme that is secure against adaptive chosen message attacks [18]. Such a scheme could be RSA [21] or ElGamal encryption [8].

Setup cookies: For each setup, the initiator sends over a *setup cookie* that is evidence of the initiator having paid a cost (or that it is possible to force him to pay this cost.) This may either be implemented using a puzzle, or by some monetary mechanism.

6 Design Principles and Solution

A first design principle is to shift the computational burden from the receiver of an email to the instigator. In order to do this, we want the setup cookie to be verifiable with a minimum of effort by the receiver. In particular, we do not want the receiver to have to perform any decryption for this to be possible, and so, since the setup cookie must be sent in cleartext, it must be specific to the sender and receiver (in order to avoid "cookie kidnappings".) Furthermore, the response should also be possible to generate with a minimum of effort, which is the reason for the *one-time response pad* we suggest. Finally, we want to minimize the amount of storage allocated by the recipient, which is done using the compacting method suggested in [12]. All together, the use of these principles reduce the risks for denial-of-service attacks mounted on potential receivers by flooding these with incorrect setup requests.

A second design principle is for valid extensions to depend on the message and be such that they cannot be forged by an eavesdropper. This corresponds to not sending the password in the clear, but to instead prove knowledge of the password, where the proof is done with respect to the message sent. This is practically achieved using MACs.

We now present our solution:

1. **Request for Setup:**
   If Sally sends an email to Ray's core address, her computer gets an automatic response with Ray's public key y_R in. Her email is not delivered, but bounces back. Along with the returning message, a homepage or ftp address may be sent, from which appropriate software may automatically be downloaded.

2. **Setup:**
   Sally's computer generates and sends a setup cookie and a one-time pad P to Ray's computer, the latter encrypted with Ray's public key y_R. Ray's computer verifies the correctness of the cookie (corresponding to verifying

that the puzzle solution or the piece of digital cash is valid), and selects a symmetric key K_{RS} uniformly at random from the set of possible keys. (We explain later how this can be performed in a way that conserves resources for Ray.) Ray adds a sufficient amount of redundancy[2] to K_{RS}, resulting in the value K'_{RS}. Ray then replies to Sally with $P \oplus K'_{RS}$ (using a publicly known extension used solely for setup). On receiving this message, Sally computes K_{RS} and verifies that no errors were introduced. She then stores (Ray, K_{RS}) in a list of all such access keys. All future emails from Sally to Ray will be processed using this key[3].

3. **Sending a message:**
   Let m be the message Sally wants to send to Ray, $\mu = hash(m)$, and let $e = MAC_{K_{RS}}(\mu)$. This value e is used as an extension of Ray's email address when the message m is sent to him.

4. **Receiving a message:**
   Ray's computer looks up (or computes) K_{RS}, given the alleged sender of the email, Sally. Ray's computer calculates e as above, and accepts the email iff the same result as in the extension is obtained. An accepted email gets delivered to Ray, just like a normal email would normally be delivered after having been received. Otherwise, the email is considered as a request for setup (see above) and the message goes undelivered.

Remark 1: Compact key management. The symmetric key can be generated by Ray as $K_{RS} = h(K_R, S, i_S)$, where h is a hash function, K_R is Ray's secret key, S is Sally's name and i_S is a sequence number that is increased for each setup request by Sally. In our model, this amounts to the same as choosing this key uniformly at random from the same set of keys. However, it allows Ray a very compact representation of the key; he merely has to store his secret key and a small counter indicating the value of i_S.

Remark 2: Message Privacy. For the message encryption we propose to use DES in the CBC mode [16]. The secret key can be generated by Sally as $K_S = h(K_{RS}, count)$[4], where h is a hash function, K_{RS} is the shared key from the MAC, and *count* is a counter increased for each message sent between

[2] The redundancy is added in order to allow the detection of third-party mounted substitution attacks. This is an attack which, if successful, manages to convince Ray that he has received a valid key from Sally, whereas he has not. This in turn will make his future messages to Sally either bounce or be discarded (depending on how the system is configured.) The redundancy adding function must be such that the resulting encryption scheme is non-malleable [7]. We suggest adding redundancy using an error detecting code. Due to space limitations, we do not, however, elaborate on how to do it.

[3] We make the simplifying assumption here that the scheme is symmetric, i.e., all future emails from Ray to Sally will use this key as well.

[4] It is also possible to use the key K_{RS}, but to achieve stronger security and easier analysis, we propose to use different symmetric keys for the two applications.

Sally and Ray. (We note that this key may be generated without any extra communication.)

Remark 3: Categorization. In the above, we have only described filtering to avoid unwanted email. It is trivial to use the same methods to categorize the incoming emails according to sender-specific categories. It is possible for a sender to request a higher (or lower) priority by indicating this in some field that gets authenticated along with the message. This is relatively safe from abuse since if a user is considered to have abused the increased priority setting he may lose his registration.

Remark 4: Use of Headers. Instead of using the format of address extensions suggested in [10], the MAC can be communicated in an available header of the email. This allows an increased transparency of the implementation.

Remark 5: An alternative implementation. Instead of using the above method in which the reply is encrypted using the previously transmitted one-time pad, we can have Sally send over a public key which is used by Ray to encrypt the symmetric key sent to Sally. In order to minimize the computation for Ray, RSA should be used for this purpose. In order to avoid the replacement of K_{RS} by a saboteur adversary, Ray could sign the key before encrypting it. All in all, this solution appears to amount to roughly the same computational expenses for Ray.

This basic protocol satisfies requirements 1-3, and requirement 4 as well for the protocol in which encryption is used to obtain message privacy. We prove these claims in the Appendix.

Acknowledgements

Many thanks to Daniel Bleichenbacher for inspiring discussions.

References

[1] M. Bellare, R. Canetti, H. Krawczyk, "Message authentication using Hash Functions-The HMAC Construction," RSA Laboratories' CryptoBytes, 1996.

[2] M. Bellare, R. Canetti, H. Krawczyk, "Keying Hash Functions for Message Authentication," Advances in Cryptology - Proceedings of Crypto'96, pp. 1-15.

[3] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation," FOCS, 1997.

[4] M. Bellare, P. Rogaway, "Random oracles are practical: A paradigm for designing protocols," First Annual Conference on Computer and Communications Security, ACM, 1993.

[5] L.F. Cranor, B.A. La Macchia, "Spam!," Communications of ACM 98. Available at `http://www.research.att.com/~lorrie/pubs/spam.`

[6] C. Dwork, M. Naor, "Pricing via Processing or Combating Junk Mail," Advances in Cryptology-Proceedings of Crypto'92, pp.139-147.

[7] D. Dolev, C. Dwork, M. Naor, "Non-malleable cryptography," STOC'92, pp. 542-552.

[8] T. ElGamal, "A Public-Key Crytosystem and a Signature Scheme Based on the Discrete Logarithm," Advances in Cryptology - Proceedings of Crypto'84, pp. 10-18.

[9] M. Franklin , D. Malkhi, "Auditable Metering with Lightweight Security," Financial Cryptography '97, pp. 151-160.

[10] E. Gabber, M. Jakobsson, Y. Matias, A. Mayer, "Curbing Junk E-Mail via Secure Classification," Financial Cryptography '98.

[11] R.J. Hall, "Channels: Avoiding Unwanted Electronical Mail," Communications of ACM '98. Available at `ftp://ftp.research.att.com/dist/hall/papers/agents/channels-long.ps`

[12] M. Jakobsson, "Mini-Cash: A Minimalistic approach to E-Commerce," PKC '99, pp. 122-135.

[13] M. Jakobsson, K. Sako, R. Impagliazzo, "Designated Verifier Proofs and Their Applications," Advances in Cryptology-Proceedings of Eurocrypt'96, pp. 143-154.

[14] A. Juels, J. Brainard, "Client Puzzles : A Cryptographic Countermeasure Against Connection Depletion Attacks," Proceedings of the 1999 Network and Distributed System Security Symposium, Internet Society, pp.151-165.

[15] NBS FIPS Pub 46-1, "Data Encryption Standard," U.S. Department of Commerce, 1988.

[16] NBS FIPS Pub 81, "DES modes of operation," U.S. Department of Commerce, 1980.

[17] NBS FIPS Pub 180-1, "Secure Hash Standard," U.S. Department of Commerce, 1995.

[18] M.Naor, M. Yung, "Public-key cryptosystems provably secure against chosen chipertext attacks," Proceedings of the 22nd Annual Symposium on Theory of Computing, ACM, 1990.

[19] B. Preneel, P. van Oorschot, "On the security of two MAC algorithms," Advances in Cryptology-Proceedings of Eurocrypt'96, pp. 19-32.

[20] R. Rivest, "The MD5 Message-Digest Algorithm," RFC1321, 1992.

[21] R.Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v.21, n.2, 1978, pp. 120-126.

[22] B. Schneier, *Applied Cryptography*.

[23] G. Tsudik, "Message authentication with one-way hash functions," ACM Computer Communications Review,v.22,n.5,1992, pp. 29-38.

A Proofs

Theorem 1: Our system protects against the *spamming attack* in the chosen message attack model. This means that we first allow an adversary E to receive valid MACs on a polynomial number of messages that E chooses. Then, if an adversary is successful in making some k non-corrupted participants $R_1 \ldots R_k$ accept each one message $M_1 \ldots M_k$, he must first pay at least a cost $(k-k')(C-\epsilon)$, where k' is the number of the above messages that are labelled as being sent by a corrupted participant, and ϵ is a small constant that corresponds to the maximum savings possible by batching several setup computations.

Proof of Theorem 1:
Let us assume that the receiver R accepts an email with the belief that it was sent by a sender S. Since the receiver is assumed not to be corrupted, he only accepts emails with valid MACs w.r.t. the believed sender. The adversary E cannot gain any information from corrupting participants not involved as sender or receiver in any of the message transfers, since the secret keys used for the MACs are chosen independently at random. (If this does not hold then the assumption that the hash function used to generate the shared secret keys is a random oracle does not hold.) Moreover E can not get any information about the secret key during its transmission, since the one-time pad is secure because its encryption protects against adaptive chosen message attacks. Therefore, the adversary must either (1) corrupt somebody who has paid the setup cost C, or (2) pay the setup cost $C-\epsilon$ for the email to be accepted, or (3) has to produce the valid MAC without the key given in the setup phase. (This is the case since no such key or portion of it will be given out without the expected setup cost C has been paid.) In the former case, S is one of the k' corrupted players, and in the second S is one of the k "paying" participants. We argue that the third case only can occur with a negligible probability. This is so since the MAC according to the assumptions is resistant against chosen message attacks. Thus, the total cost paid by the adversary is $(k-k')(C-\epsilon)$. □

Theorem 2: Our system protects against the *authentication attack*, i.e., the adversary is not able to make a receiver R accept an email M and present this to the user as originating from a non-corrupted participant S, when in fact the message did not originate from S.

This follows from the proof of Theorem 1, and the fact that non-corrupted participants will only accept emails with valid MACs corresponding to the apparent sender.

Theorem 3: Our system protects against the *sender privacy attack*, i.e., an adversary is not able to convince a non-corrupted participant E that a message M was sent by a non-corrupted sender S to some (potentially corrupted) receiver R.

Proof of Theorem 3: Due to the property that the MACs are assumed secure against a chosen message attack, it is not possible for a third party to determine that a given message was sent by one of R and S (without attempting to determine which one) without the involvement by either of these two parties. Let us therefore assume that one of these two parties collaborates with the third party to try to convince the latter that the other participant sent a certain message. If M was sent from S to R than it has a valid extension computed with the correct key K_{RS}. However, this key is also known to R, and thus, it is not possible to determine whether R or S originated the message. Therefore, if one of the participants were to try to convince a third party of who the sender is, the third party will not trust the proof, as the transcript could have been computed by either R or S. □

Theorem 4: If the encryption mode of our scheme is employed, then our system protects against the *message privacy attack*, i.e., the attacker is not able to determine whether a first message M_1 or a second message M_2 was sent between two non-corrupted participants.

This follows directly from the symmetric cipher being assumed to be secure against chosen message attacks.

SUBMISSION NO. : 118626

ATTORNEY : Weinick, Jeffrey M.

Title :
How To Protect Against A
Militant Spammer

-------------------MAIN INFORMATION--------------------

ITEM STATUS	: Opened	LUCENT RATING	:
STATUS DATE	: 04/23/1999	PATENT WPN	: U0
OPEN DATE	: 04/05/1999	GOVT. CONTRACT	: No
CLOSE DATE	:	TYPE	: Patentability
DEADLINE DATE	:	DEFENSIVE	: No
BU CODE(S)	: BLRS,OUTSIDE		

-----------------SUBMITTER INFORMATION-----------------

SUBMITTER NAME	: Jakobsson, Bjorn Markus
COMPANY	: LUCENT
LOC_EXT	: 908-582-8138
DEPARTMENT	: BL0112350
DIRECTOR	: A. Silberschatz

SUBMITTER NAME	: Mueller, Joy Colette
COMPANY	: UMAINZ
LOC_EXT	:
DEPARTMENT	: OUTSIDE
DIRECTOR	:

Brief Description :

No data in this field

EXHIBIT B

Lucent Technologies
Bell Labs Innovations

Bell Laboratories

Subject: **How to Protect Against a Militant Spammer**

date: **April 2, 1999**

from: **A. Silberschatz**
Org. BL0112300
MH 2T-310
908-582-4623

J. Weinick:

Jeff:

Please consider the patentability of the attached "How to Protect Against a Militant Spammer". The following is a description of the patentable part of the paper.

Several methods exist to prevent against spamming performed by an attacker who buys email addresses or gets such from newsgroups. None exist that also protect against attackers who can eavesdrop on communication lines and/or alter messages sent by others.

We protect against the above mentioned adversary, shift computational costs towards initiators of traffic, and implement additional properties such as authenticity and encryption for no extra cost or for a low extra cost, given the existing architecture to prevent against spam.

I propose design methods to shift costs towards initiator; use known MAC methods in a new way in order to prevent against the spamming attack. The former puts a well-known primitive, the one-time pad, to a novel use; whereas the latter uses MACs to communicate passwords in a way that prevents these from being stolen.

A strong intellectual property position in this regard will be of immense value to Lucent.

ml
MH-BL0112350-MR-aa

A.
A. Silberschatz

Attachment

EXHIBIT C

Lucent Technologies

Request for Approval of Manuscript

BL99.00549

To:

PATENT
Suggested reviewer: J. Weinick

Date: April 7, 1999

Please review and return (or **FAX 732-949-2822**) before **April 28, 1999.**

for a talk intended for presentation at
Communications and Multimedia Security
Leuven, Belgium
September 20, 1999

Intended for publication in
Proceedings of Communications and Multimedia Security

Title: How to Protect Against a Militant Spammer

Authors	Company	Tel.	Loc.	Room	Org.
Jakobsson, B.M.	LU	(908) 582-8138	100001	2A-362	10009634
Muller, J	Universitat Mainz		Mainz		

Reviews:

The following individual(s) have been notified of the intention to release this material:
PATENT - Suggested Reviewer: J. Weinick

Additional Information:

The author's organization has answered the following questions as indicated:
* Is any of the work discussed supported by government funds? **no**

Abstract:

We consider how to avoid unsolicited email - so called spam - in a stronger adversarial model than what has previously been considered. Our primary concern is the proposal of an architecture and of protocols preventing against successful spamming attacks launched by a strong attacker. This attacker is assumed to control the communication media and to be capable of corrupting large numbers of protocol participants. Secondly, we show how services such as message integrity and message privacy can be obtained virtually for free by using the structures put in place for spam protection. A final issue we are concerned with is how to produce protocols that have the property that the bulk of the computational requirements and storage requirements are shifted towards one of the participants, in order to reflect the desired power balance and to avoid denial-in-service attacks. This results in a simple and efficient solution that is largely backwards-compatible, and which addresses many of the concerns surrounding email communication.

Recommendation:

☑ **Approved**

SEND ALL COMMENTS DIRECTLY TO FIRST Lucent Technologies AUTHOR

□ **ON HOLD until further notice:** I will discuss issues with author.

Patent Attorney 4/21/99
Date

Please return to: Publication Clearance Service - Lucent Technologies
Room 1A-127, Crawfords Corner Rd., Holmdel, NJ 07733-3030
(732) 949-0241

EXHIBIT D

Lucent Technologies
Bell Labs Innovations

Eli Weiss
Corporate Counsel
Intellectual Property-Law

101 Crawfords Corner Road
Room 3K-206
Holmdel, NJ 07733-3030 USA

Telephone 732 949 3147
Facsimile 732 949 0292
E Mail holawa!ew

May 21, 1999

VIA EXPRESS MAIL

Lance Lieberman, Esq.
Cohen, Pontani, Lieberman & Pavane
551 Fifth Avenue
New York, NY 10176

Re: **IDS No.:** 118626

Managing Attorney	**Telephone No.**	**Fax No.**
Jeffrey M. Weinick	(908) 582-2188	(908) 582-4020
Secretary	**Telephone No.**	
Deborah B. Cornish	(908) 582-6824	

Dear Lance:

The above referenced patent submission is enclosed with this letter. ***This case relates to Gabber 8-1-18-4, a copy of which is enclosed for your information.*** Prior to contacting the authors of the submission, please call the Managing Attorney identified above for his thoughts and instructions.

NOTE: This case **MUST** be filed by **September 20, 1999.** **THE DATE IS CRITICAL as it may be disclosed during a talk in Belgium on September 20, 1999.** Please call the Managing Attorney to confirm that this case will be filed by the critical date. If, for any reason you cannot meet that date, you MUST notify the Managing Attorney and me, VIA FACSIMILE, as soon as possible. If the Managing Attorney and you agree to change the date to file, confirmation VIA FACSIMILE must be sent to the Managing Attomey and to me for our records.

As soon as you have identified the inventors, please send Attachment H (Request for Case Name/Number) via facsimile to Norma Davis (732) 949-0292. After the application is completed, but before the Declaration and Assignment are executed, please send a copy to the Managing Attomey for his review and instructions to proceed. The completed application is to be mailed from your office directly to the USPTO. A copy of all papers sent to the USPTO should be sent to Norma Davis for our files, together with the debit note for preparing the patent application.

Very truly yours,

E L Weiss

Eli Weiss
Corporate Counsel

EW: nmd

Encl. (As above)

Copy to:
J.M. Weinick
B.M. Jakobsson
J.C. Mueller

EXHIBIT E

COHEN, PONTANI, LIEBERMAN & PAVANE

551 Fifth Avenue New York, New York 10176-1022

TELEFAX TRANSMITTAL

October 15, 1999

To: Bjorn M. Jakobsson Fax#: 908-582-~~8138~~ 1239

From: Jeffrey M. Navon, Esq. Fax#: (212) 972-5487

Re: IDS 118626, How to Protect Against
A Militant Spammer

Confidentiality Statement

This transmission may contain information which is legally privileged or otherwise protected from disclosure. Its contents are confidential and intended for the addressee only, and must not be used, copied or disseminated by any person other than the addressee. The recipient is requested to notify the sender immediately of any error in transmission and to destroy any transmission not intended for the recipient.

23 Pages Follow This Cover Sheet

If all pages are not received
Or you experience other transmission difficulties
Please call us at (212) 687-2770

Confirmation will follow
X Confirmation will not follow

Dear Mr. Jakobsson:

We have been retained by Lucent to prepare a draft patent application in the above referenced matter. I have prepared such a draft based on the IDS and the paper which you authored. I found the paper to be very helpful, highly readable and informative. Please review this draft at your convenience and get back to me with any comments that you may have. Please also share the draft with Ms. Mueller, your coinventor. I can be reached at (212) 687-2770 and at JEFFREY@cplplaw.com.

Thank you for your attention to this matter.

Best regards.

EXHIBIT F

Lance Lieberman

From: Jeffrey M Navon
Sent: Tuesday, December 07, 1999 10:35 AM
To: Lance Lieberman
Cc: Myron Cohen
Subject: RE: Outstanding Lucent applications

Hello Lance:

I didn't realize you were able to check your email from Taiwan so was going to give you an update when you came back. But, here it is anyway.

Cases -193 and 207 have been filed.

Cases 202 and 225 are with the managing attorney for approvals to file.

I spoke the inventor in case 238 and he said it was in good shape but wanted to read through it once more and would get back to me within the week.

I received comments from the inventor in case 242 late last week and have made the revisions and will send it back out for another review this week.

I spoke to the inventor in cases 236 and 237 (related cases) and he said he would finish his review by December 15.

The inventor in case 186 is waiting for one more inventor to sign the papers and send it back to us. This group of inventors is the most dilatory and I spoke to Greg Murgia (managing attorney) to see if he could move it along.

Hope you are enjoying your trip.

Jeff

> -----Original Message-----
> **From:** Lance Lieberman
> **Sent:** Tuesday, December 07, 1999 9:56 AM
> **To:** Jeffrey M Navon
> **Cc:** Myron Cohen
> **Subject:** Outstanding Lucent applications
> **Importance:** High
>
> On 11/24, before I left for Taiwan, I sent you several e-mails on nine Lucent cases that you've worked on and that have yet to be billed or, apparently, filed in the PTO.
>
> These cases are 4167-186/193/202/207/225/236/237/238/242. Your entered time on a number of these cases goes back to January of 1999! All of them should have been filed, at the very latest, by several months ago under Lucent's instructions.
>
> In my e-mails of 11/24, I asked you to contact the inventors and Managing attorneys if we're just waiting for the papers to be approved or executed for filing, and to put your requests in writing so that we can show Lucent that the delay is not on our end. I also asked you to advise me asap of where we stand with these cases, and of what steps you've taken toward getting them filed per my above request. These nine cases represent $50,000 worth of billing, and I want to be sure that they're filed and billed by the end of the year.
>
> To date, I've received no response from you, though I've been checking my e-mail daily. Please let me hear from you on these NOW. concerning any of these cases

EXHIBIT G

Lucent Technologies
Bell Labs Innovations

Jeffrey M. Weinick
Corporate Counsel
Intellectual Property - Law

600-700 Mountain Avenue
Room 3B-507
P.O. Box 636
Murray Hill, NJ 07974-0636 USA

Telephone 908 582 2188
Facsimile 908 582 4020
E Mail jweinick@lucent.com

February 9, 2000

Mr. L. Lieberman
Cohen, Pontani, Lieberman & Pavane
551 Fifth Avenue
New York, NY 10176

Re: IDS No. 118626

4167-242 (JMK)

Dear Mr. Lieberman:

A review of my outside counsel docket has revealed that the above referenced patent submission, which was originally due to be filed on September 20, 1999, and for which no filing date extension has been granted, has not yet been filed.

Considering the age of this submission, a new **non-extendible** filing deadline of **March 30, 2000** is being set for this case. Of course, this presumes that there is no statutory bar date prior to the new filing deadline. Ultimate responsibility for filing before any such bar date rests with you.

If you are having difficulties obtaining the necessary information from the inventors, or if you have encountered any other exceptional circumstances, please contact me at the above telephone number.

Please sign the acknowledgment below and return this form to me, via facsimile, as soon as possible.

Very truly yours,

Jeffrey M. Weinick

Jeffrey M. Weinick

Filing Date Acknowledged:

________________________ Date: ________________
L. Lieberman

Copy to
B. M. Jakobsson
J. C. Mueller

EXHIBIT H

Jeffrey M Navon

From: Markus Jakobsson [markusj@research.bell-labs.com]
Sent: Friday, March 10, 2000 4:43 AM
To: jeffrey@cplplaw.com
Subject: comments

Jeff,

I have read your update on the spam patent application.
Some comments:

✓p 12 line 6 "one-time pad P" -> "using a stream cipher generated pad P"

✓p 15 l 16 "senders-specific" -> "sender and receiver specific"

✓claim 2: the address is not encrypted. Do you mean the MAC result? that can be sent as an extension to the email address that is peeled off

by the gateway. You can also use special fields for additional info to transmit the MAC portion.

✓ claim 3: again: no encrypted address. Do you mean later on that the message would also be encrypted, or do you refer to the MAC? Let's call the MAC result something like an "identifyer" to seperate it from standard encryption, and avoid confusion.

✓claim 4. not over a public key, but "using public key encryption"

✓ figs after 120, the resulting email would be bounced. the sender would attach the "cost item" and send it again (this could be done automatically)
and when it comes again (no state needs to be kept by the recipient) then the recipent would handle it like a new incoming email.

– add [illegible] 165, 166. 168

✓also, 80, I am not sure what you mean here. is that out of band? normally you have to know the core address of the person you want to talk to.

Give me a call if you need to clarify and discuss.
Cheers,
Markus

EXHIBIT I

Jeffrey M Navon

From: Markus Jakobsson [markusj@research.bell-labs.com]
Sent: Wednesday, March 22, 2000 9:54 AM
To: Jeffrey M Navon
Subject: Re: Spam Patent Application

Hi Jeff,

I have looked at the fax now. A few more comments, then I think we are done ✓
(you don't need to send it to me once these are corrected, but I think it is
ready to
file then.)

page 14 "is preferrably a generated pseudorandom function that uses" -> ✓
"is preferrably generated using a psuedorandom function, e.g., "

page 14 "other number generators" -> "other methods of generating identifiers" ✓

claim 1: I am concerned that this would not be allowed, given Gabber et al. (No ✓, ignored
What do you think?

fig 2 "one time pad" -> "a key or pad" ✓

Cheers,
Markus

EXHIBIT J

COHEN, PONTANI, LIEBERMAN & PAVANE
COUNSELLORS AT LAW
PATENTS, TRADEMARKS & COPYRIGHTS
551 FIFTH AVENUE
NEW YORK, NEW YORK 10176

TEL: (212) 687-2770
FAX: (212) 972-5487

MYRON COHEN
THOMAS C. PONTANI, PH.D.
LANCE J. LIEBERMAN
MARTIN B. PAVANE
MICHAEL C. STUART
WILLIAM A. ALPER
KLAUS P. STOFFEL

EDWARD M. WEISZ
CHI K. ENG
YUNLING REN, PH.D.
JULIA S. KIM
MINDY CHETTIH
VINCENT M. FAZZARI
CATRIONA M. COLLINS
ALFRED W. FROEBRICH
ALFRED H. HEMINGWAY, JR.
ANDRES N. MADRID
JEFFREY M. NAVON*
KENT H. CHENG, PH.D.
TZVI HIRSHAUT

*Not admitted in New York

April 3, 2000

VIA EXPRESS MAIL

EL489905156US

Ms. Susan E. Curry
Administrative Manager
Lucent Technologies Inc.
IP-Law, Outside Counsel Group
Room 3K-201
P.O. Box 3030
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

Re: New U.S. Patent Application
For: **Methods of Protecting Against Spam Electronic Mail**
Case No.: **Jakobsson 22-2** - IDS No. 118626
Our File No.: **4167-242**

Dear Susan:

This is to confirm the March 30, 2000 filing of the above-identified patent application in the United States Patent and Trademark Office. Copies of the application with accompanying drawings, the transmittal letter and the unexecuted Declaration are enclosed for your files. We also enclose a 3½" floppy disk containing a copy of the application in Word 6 format.

As the application was filed in unexecuted condition, we are forwarding a copy of the application with the Declaration and Assignment to the inventors for execution at this time.

The drafting vendor for this application is Drafting by Design. Informal drawings were submitted with this application.

If you have any questions, please do not hesitate to contact us. Pursuant to your request, our debit note is enclosed.

Very truly yours,
COHEN, PONTANI, LIEBERMAN & PAVANE

Lance J. Lieberman

LJL/jp
Enc.

RELATED PROCEEDINGS APPENDIX

None.